Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security®
By
Chris Bester

On August 24, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google products and active exploitation of vulnerabilities affecting Apple and Mozilla products.
CIS Security Advisories

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

26 August 2022

In The News This Week

The governments of Ukraine and Poland signed a memorandum on cooperation in the field of cyber defense - Today, (2022-08-22), the Ministry of Digital Transformation of Ukraine, State Special Communications, and the Office of the Prime Minister of the Republic of Poland signed a memorandum of understanding in the field of cyber protection. Since the beginning of the full-scale invasion of Ukraine, Russian hackers have also repeatedly attacked Poland. The signing of this document is an important step toward joining forces to repel the enemy in cyberspace. "The first world cyber war is happening now. Therefore, joining forces and exchanging practices is a logical step in this area. With Poland, we have not only a common physical border but also common problems in cyberspace, where we are subjected to the same attacks. I am sure that together in this struggle, we will become stronger and more effective", – Mykhailo Fedorov, Deputy Prime Minister – Minister of Digital Transformation of Ukraine. The memorandum will strengthen the joint fight against cybercrime and make exchanging experience and information about cyber incidents faster and more efficient. "Cyber defense is not created alone. It is always a joint effort…" Read the rest of the post here: Odessa Journal

Lloyd's to exclude certain nation-state attacks from cyber insurance policies
Lloyd's of London insurance policies will stop covering losses from certain nation-state cyber attacks and those that happen during wars, beginning in seven months' time. In a memo sent to the company's 76-plus insurance syndicates, underwriting director Tony Chaudhry said Lloyd's remains "strongly supportive" of cyber attack coverage. However, as these threats continue to grow, they may "expose the market to systemic risks that syndicates could struggle to manage," he added [PDF], noting that nation-state-sponsored attacks are particularly costly to cover. Because of this, all standalone cyber attack policies must include "a suitable clause excluding liability for losses arising from any state-backed cyberattack," Chaudhry wrote. These changes will take effect beginning March 31, 2023 at the inception or renewal of each policy…
Read the full story by Jessica Lyons Hardcastle here : The Register

Hackers Are Breaking Into and Emptying "Cash App" Accounts
Multiple users of the hugely popular Cash App have reported hackers stealing their funds, and fraudsters are selling access to accounts on the dark web. - Hackers are breaking into unsuspecting victims' Cash App accounts, a massively popular payment app, and stealing hundreds of dollars, according to victims Motherboard spoke to. In one person's case, they said, Cash App has not reimbursed them for the stolen funds. "It's scary!" Liz Shelby, who said their son was a victim of the hacking, told Motherboard in an online chat. "My son saved up some cash for a small vacation with his grandma. We put it in his Cash App before he left. He called me on Aug. 9, and told me that his money was gone." Shelby said that after she looked at the account she found that someone else had logged into it and sent themselves the money. Shelby said she's been emailing Cash App support, without success. "I'm not getting anywhere and I'm sure my son will never get his money back," she added. Cash App is one of the most popular payment services apps, with over 50 million downloads from the Google Play Store. Read the rest by Joseph Cox here: Vice

Nato investigates hacker sale of missile firm data
Nato is assessing the impact of a data breach of classified military documents being sold by a hacker group online. - The data includes blueprints of weapons being used by Nato allies in the Ukraine conflict. Criminal hackers are selling the dossiers after stealing data linked to a major European weapons maker. MBDA Missile Systems admitted its data was among the stash but claimed none of the classified files belong to the firm.
The pan-European company, which is headquartered in France, said its information was hacked from a compromised external hard drive, adding that it was cooperating with authorities in Italy, where the data breach took place.." Read the rest of the article here: BBC News

Google blocks third record-breaking DDoS attack in as many months
46 million requests per second network flood comes as attacks increase by more than 200% compared to last year. - Google says it has blocked the largest ever HTTPS-based distributed-denial-of-service (DDoS) attack in June, which peaked at 46 million requests per second. To put things in perspective, this is about 76 percent larger than the previous record DDoS attack that Cloudflare thwarted earlier that same month. As Googlers Emil Kiner and Satya Konduru explain: "That is like receiving all the daily requests to Wikipedia (one of the top 10 trafficked websites in the world) in just 10 seconds."These types of security events flood target organizations' networks with junk traffic, which makes it impossible for them to conduct legitimate business online. Not only is this the third such record-breaking DDoS flood in the past few months – this includes two earlier HTTPS-based attacks blocked by Cloudflare in April and June – but it comes as Google and other security researchers warn that network-flooding events are getting worse, growing in size and frequency. Read the full story by Jessica Lyons Hardcastle here: The Register

Estonia Repels Biggest Cyber-Attack Since 2007
The Estonian government has revealed that the country was on the receiving end of the "most extensive" DDoS attacks in 15 years this week after angering Moscow. The former Soviet state reportedly removed a Red Army monument from Tallin square this week, while a Soviet-era tank was removed in the eastern city of Narva. The government has pledged to take down hundreds of such monuments by the end of the year following Russia's invasion of Ukraine. In response, pro-Russian cybercrime group Killnet has reportedly claimed responsibility for launching a series of DDoS attacks against the websites of public and private sector organizations. Estonian government CIO, Luukas Ilves, took to Twitter to dismiss the group's claims that more than 200 sites had been floored. "The attacks were ineffective. E-Estonia is up and running. Services were not disrupted. With some brief and minor exceptions, websites remained fully available throughout the day. The attack has gone largely unnoticed in Estonia," he said. "As Government CIO, I slept well." Read the rest of the article by Phil Muncaster here: InfoSecurity

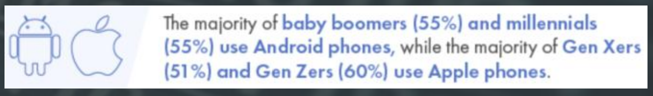
Cybersecurity: Apple vs. Android

Probably one of the most asked security questions if it comes to mobile devices is "which phone or OS is more secure, Apple or Android?". If you wander through the Internet forest, it seems that Apple users believe they are more secure but almost the same number of Android users feel the same about Android. So, what is it then? Beyond Identity did a survey last month asking the same question, and I thought it would be apt to share the blog with you this week. Below then is an extract of the survey findings.

Apple vs. Android

A sense of security is often a driving force behind decision making, but how much weight does it hold when selecting a phone? Though Android smartphones dominate the global market, the U.S. has been historically partial to iPhones. With privacy concerns mounting worldwide, the team at Beyond Identity decided to speak to over a thousand Americans to see how secure they felt with their Apple and Android devices.

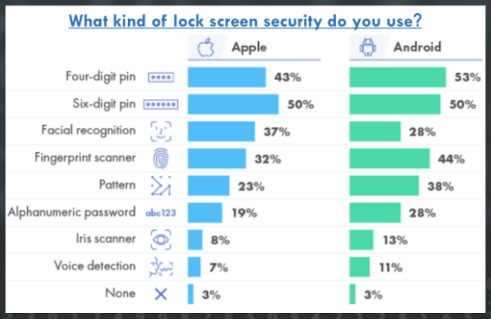
How often have iPhone users been hacked compared to Android users? Which subset is thinking of making the switch because of security? And which consumers are exhibiting generally safer behavior, regardless of how their phone operates? If you're questioning your phone choice or looking for experienced users to weigh in, you're in the right place.


The majority of baby boomers (55%) and millennials (55%) use Android phones, while the majority of Gen Xers (51%) and Gen Zers (60%) use Apple phones.

How safe do users feel? - The study began with an initial pulse check into how iPhone and Android users feel about the security of their devices. We also found out what Americans had to say about using the data storage services offered by iCloud and Google.

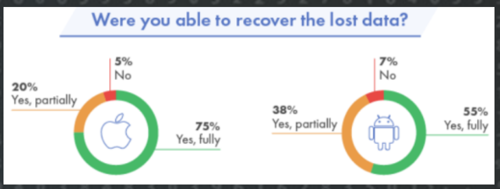
According to the users of each type of smartphone, the iPhone 13 Pro Max felt remarkably safer than the Samsung Galaxy S22 Ultra. In fact, iPhone 13 users were more than twice as likely to say that theirs was the most secure smartphone they had ever used.

Smartphones weren't the only pieces of tech where Apple users reported a heightened sense of security. Apple iCloud Keychain (the company's password storing app) users were seven percentage points more likely than Google Password Manager users to feel "extremely" secure about their password storage method. Still, there's an inherent risk to the convenience of password storing—and even using a password in the first place—compared to more secure passwordless solutions.



In perhaps one of the most convincing statistics, current Android users in the US are highly likely to consider switching to Apple, specifically because of updated security features. Of the Android users considering the switch to Apple, nearly half (49%) cite the perceived security and privacy superiority of Apple's operating systems as the main reason.

While newly released operating systems often come with improved security features, Apple's upcoming release of iOS 16 is what led 33% of Android users to consider switching to Apple. The release introduces extreme security features designed to protect users from highly targeted mercenary spyware, including "Lockdown Mode," which strictly limits or completely shuts down apps and protocols that can put the user at risk of cyber attack.



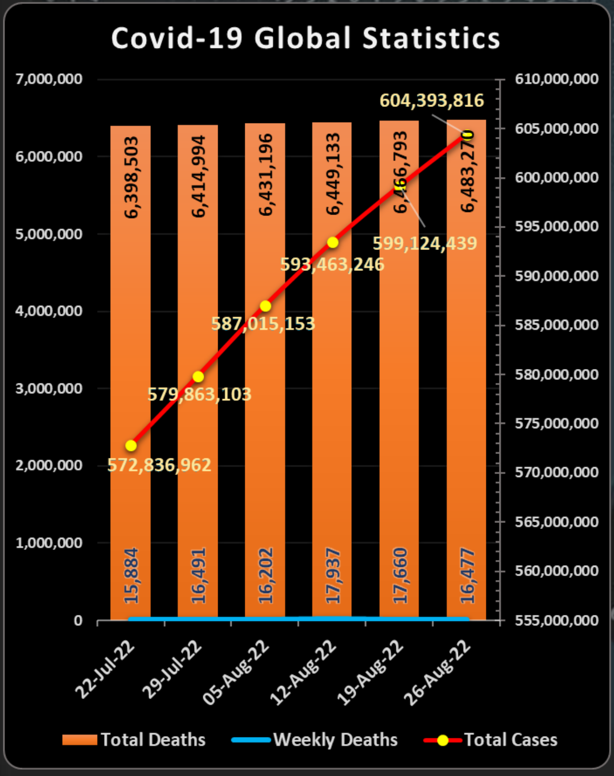
Data Breaches - In this last piece of our study, we asked respondents to share their experiences with security breaches on their iPhones and Androids. We also asked about how well they were able to recover information and finances after these unfortunate events occurred. Neither Apple nor Android users were strangers to hacks and security breaches: 40% or more of both groups had experienced malware attacks or cyber scams. However, Apple once again had the advantage: More of their users reported never experiencing a security breach of any kind. And when breaches did happen, they were 20 percentage points more likely to fully recover the data they had lost compared to Android users.
However, Apple users may have felt a little too safe as they were more likely to report regularly losing their phones—often as many as six or more times in the last six months. This may have to do with what's known as the Peltzman Effect, which theorizes that when safety measures are in place, people are more likely to take risks.

Settling the great security debate
Despite the massive financial and market-share-based success of Android phones, the iPhone reigned supreme in terms of security according to users. People with iPhones reported fewer breaches and more instances of retrieving their stolen or lost information.

Apple users are also more careful with their information. They used longer passwords and disabled their location services more often than Android users, many of whom reported wanting to switch to the iPhone for security purposes. So, if you're in the market for a new phone and security is a top concern, you may want to heed the experiences of over 1,000 smartphone users.

Resources: Beyond Identity, See another review by MakeUseOf, and yet another review by Trusted Reviews

Covid-19 Global Statistics



For Reporting Cyber Crime in the USA go to **(IC3)** , in SA go to **Cybercrime**, in the UK go to **ActionFraud**

Other Interesting News and Cyber Security bits:

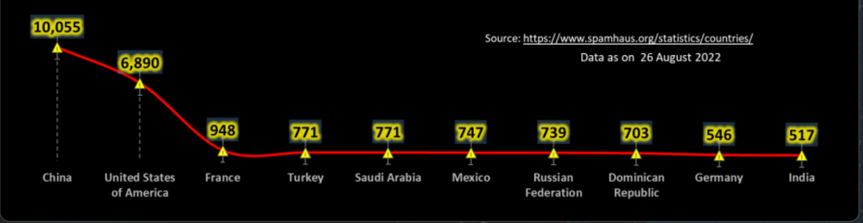
- Janet Jackson music video declared a cybersecurity exploit
- Lincoln Model L100 autonomous concept car unveiled (No Steering wheel)
- CERN- Preparing for a more powerful particle accelerator
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally

SatelliteXplorer
Track satellites in orbit

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)



Source: https://www.spamhaus.org/statistics/countries/
Data as on 26 August 2022

AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com